Remarks/Arguments

Claims 2-7, 10-24, 27 and 30-32 are currently pending in the application. Claims 14, 15, 16, 17, 23, and 24 have been amended.

Claims 14, 15, 16, 17, 21, 23, 24, and 31 stand rejected under 35 U.S.C. 112, second paragraph for being indefinite. The instant amendment of the claims deletes the phrase "is hard" from the claims. Additionally, the Applicants submit that the expression "group [P]" is not indefinite but is an expression that is clearly defined in abstract algebra such that one skilled in the art readily understands its meaning. Attached as Exhibit A is page 75 from the Handbook of Applied Cryptography which provides the accepted definition for a group. In view of the above, it is submitted that Claims 14, 15, 16, 17, 21, 23, 24, and 31 particularly point out and distinctly claim the subject matter to which the invention is directed.

Claim 7 stands rejected under 35 U.S.C. 103(a) as being anticipated by Cordery (6,175,827) in view of Vanstone (6,212,281). This rejection is respectfully traversed.

The Examiner admits that Cordery does not teach or suggest that the private key of the first party is generated as a function of the certificate, information specifying attributes of the article and the private key of the CA. However, it is the Examiner's position that Vanstone teaches this missing element. The Applicants submit that Vanstone does not teach or suggest the above method of calculating or deriving the private key of the first party. Rather, in Vanstone a message is encrypted using an encryption key derived from the short term public key r. The claimed invention does not encrypt the message this way. Additionally, in Vanstone the certificate is optionally used to provide necessary redundancy and is included in the encrypted message. In the claimed invention the certificate is not encrypted. In view of the above, it is submitted that claim 7 is not rendered obvious by the combination of Cordery and Vanstone.

Appln. No.: 09/280,528
Amdt. Dated January 15, 2004
Reply to Office Action dated January 6, 2004

It is submitted that the application stands in condition for allowance. Reconsideration of the rejections is respectfully requested and an early notice of allowance earnestly solicited. If the Examiner has any additional questions, please contact the undersigned at the number below.

Respectfully submitted,

Steven J. Shapiro
Reg. No. 35,677
Attorney of Record
Telephone (203) 924-3880

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000

EXHIBIT A
To Amendment dated 10/30/03
Appl. #09/280,528

Exhibit A

2.159 Example (*Blum integer*) For the Blum integer $n = 21$, $J_n = \{1, 4, 5, 16, 17, 20\}$ and $\widetilde{Q}_n = \{5, 17, 20\}$. The four square roots of $a = 4$ are 2, 5, 16, and 19, of which only 16 is also in Q_{21}. Thus 16 is the principal square root of 4 modulo 21. □

2.160 Fact If $n = pq$ is a Blum integer, then the function $f : Q_n \longrightarrow Q_n$ defined by $f(x) = x^2 \bmod n$ is a permutation. The inverse function of f is:

$$f^{-1}(x) = x^{((p-1)(q-1)+4)/8} \bmod n.$$

2.5 Abstract algebra

This section provides an overview of basic algebraic objects and their properties, for reference in the remainder of this handbook. Several of the definitions in §2.5.1 and §2.5.2 were presented earlier in §2.4.3 in the more concrete setting of the algebraic structure $\mathbb{Z}_n^*$.

2.161 Definition A *binary operation* $*$ on a set S is a mapping from $S \times S$ to S. That is, $*$ is a rule which assigns to each ordered pair of elements from S an element of S.

2.5.1 Groups

2.162 Definition A *group* $(G, *)$ consists of a set G with a binary operation $*$ on G satisfying the following three axioms.

(i) The group operation is *associative*. That is, $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
(ii) There is an element $1 \in G$, called the *identity element*, such that $a * 1 = 1 * a = a$ for all $a \in G$.
(iii) For each $a \in G$ there exists an element $a^{-1} \in G$, called the *inverse* of a, such that $a * a^{-1} = a^{-1} * a = 1$.

A group G is *abelian* (or *commutative*) if, furthermore,

(iv) $a * b = b * a$ for all $a, b \in G$.

Note that multiplicative group notation has been used for the group operation. If the group operation is addition, then the group is said to be an *additive* group, the identity element is denoted by 0, and the inverse of a is denoted $-a$.

Henceforth, unless otherwise stated, the symbol $*$ will be omitted and the group operation will simply be denoted by juxtaposition.

2.163 Definition A group G is *finite* if $|G|$ is finite. The number of elements in a finite group is called its *order*.

2.164 Example The set of integers $\mathbb{Z}$ with the operation of addition forms a group. The identity element is 0 and the inverse of an integer a is the integer $-a$. □

2.165 Example The set $\mathbb{Z}_n$, with the operation of addition modulo n, forms a group of order n. The set $\mathbb{Z}_n$ with the operation of multiplication modulo n is not a group, since not all elements have multiplicative inverses. However, the set $\mathbb{Z}_n^*$ (see Definition 2.124) is a group of order $\phi(n)$ under the operation of multiplication modulo n, with identity element 1. □

EXHIBIT A
To Amendment dated 10/30/03
Appl. #09/280,528

Library of Congress Cataloging-in-Publication Data

Menezes, A. J. (Alfred J.), 1965–
Handbook of applied cryptography / Alfred Menezes, Paul van Oorschot, Scott Vanstone.
p. cm. – (CRC Press series on discrete mathematics and its applications)
Includes bibliographical references and index.
ISBN 0-8493-8523-7 (alk. paper)
1. Computers--Access control--Handbooks, manuals, etc.
2. Cryptography--Handbooks, manuals, etc. I. Van Oorschot, Paul C.
II. Vanstone, Scott A. III. Title. IV. Series: Discrete mathematics and its applications.
QA76.9.A25M463 1996
005.8'2--dc20

96-27609
CIP

International Standard Book Number 0-8493-8523-7
Library of Congress Card Number 96-27609
Printed in the United States of America 1 2 3 4 5 6 7 8 9 0
Printed on acid-free paper